TURBIN CHU HEIDT, A Law Corporation
Richard Turbin (1044)
Janice D. Heidt (8984)
737 Bishop Street, Suite 2730
Honolulu, Hawaii 96813
richturbin@turbin.net
jheidt@turbin.net
Telephone: 808-528-4000
Facsimile: 808-599-1984

STRANCH JENNINGS & GARVEY PLLC
J. Gerard Stranch, IV
Grayson Wells
2233 Rosa L. Parks Ave., Ste. 200
Nashville, TN 37203
gstranch@stranchlaw.com
gwells@stranchlaw.com
Telephone: (615) 254-8801

Attorneys for Plaintiff MICHAEL LUTH
and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

| | |
|---|---|
| MICHAEL LUTH, individually and on behalf of all others similarly situated<br><br>*Plaintiffs*,<br><br>v.<br><br>HAWAII RADIOLOGIC ASSOCIATES, LTD.,<br><br>*Defendant*. | CIVIL NO. _____<br>(Other Personal Injury)<br><br>**CLASS ACTION COMPLAINT**<br><br>JURY TRIAL DEMANDED |

# CLASS ACTION COMPLAINT

Plaintiff Michael Luth ("Plaintiff"), brings this Class Action Complaint against Defendant Hawaii Radiologic Associates, Ltd. ("Defendant"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

## INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the protected health information ("PHI") of Plaintiff and other similarly situated patients of Defendant totaling tens of thousands of individuals ("Class Members"), including their names, dates of birth, health insurance subscriber ID, types of exams, and the indications resulting from those examinations.

2. According to Defendant, it became aware of suspicious activity on its information systems on August 26, 2024, and then later determined that a threat actor or group had gained access to its information systems between August 20 and August 25, 2024.[1]

3. As part of the notice, Defendant instructed affected persons to take

[1] Hawaii Radiologic Associates, *Notice of Data Event* (Oct. 25, 2024), https://www.hirad.com/updates/notice-of-data-event.

certain steps to protect themselves: "HRA encourages potentially affected individuals to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should be promptly report to their insurance company, health care provider, or financial institution."[2]

4. Defendant's notice contained little information regarding the nature of the Data Breach and its underlying cause, but it was likely caused by Defendant's failure to implement reasonable cybersecurity measures.

5. Indeed, Defendant's lax cybersecurity program is apparent because it failed to detect the malicious activity for more than five days while the threat group roamed around its infrastructure, performing the necessary and noisy reconnaissance tasks, exfiltrating files and data, and culminating in what appears to be a ransomware attack through which the hackers announced their presence to Defendant.

6. Thus, because Defendant's systems were incapable of detecting the hackers before they deployed their ransomware, it is likely that Defendant failed to implement the reasonable logging, monitoring, and alerting tools that are necessary to timely detect such malicious activity and that are basic elements of a reasonable cybersecurity program.

7. Moreover, Defendant was fully aware of the risks associated with a

[2] *Id.*

failure to implement reasonable cybersecurity measures as it appears to have experienced a similar attack two years ago that resulted in Defendant having to turn patients away.[3]

8. Here again, Defendant was required to cancel appointments and turn patients away because of a cyberattack called "reminiscent" of the 2022 event.[4]

9. Because of Defendant's failures and its inability to learn from past failures, Plaintiff and the proposed Class Members have suffered a severe invasion of privacy and are now must face years of a substantial increase in risk of identity theft and fraud, including medical and health insurance fraud.

## PARTIES

10. Plaintiff Michael Luth is a natural person and a citizen of Hawaii, though he has plans to move to Arizona where he has recently visited and placed on offer on a home.

11. Defendant Hawaii Radiologic Associates is organized under the laws of Hawaii with its principal place of business in Hilo, Hawaii.

---

[3] Dave Pearson, *Evident Cyberattack Brings Hawaii Radiology Practice to its Knees* (Nov. 4, 2022), https://radiologybusiness.com/topics/patient-care/evident-cyberattack-brings-hawaii-radiology-practice-its-knees; Grant Phillips, *Hawaii Radiologic at a Standstill*, WEST HAWAII TODAY (Nov. 3, 2022), https://www.westhawaiitoday.com/2022/11/03/hawaii-news/hawaii-radiologic-at-a-standstill.

[4] John Burnett, *Hawaii Radiologic Shut Down by 'Security Incident'*, WEST HAWAII TODAY (Sept. 18, 2024), https://www.westhawaiitoday.com/2024/09/18/hawaii-news/hawaii-radiologic-shut-down-by-security-incident.

## JURISDICTION AND VENUE

12. The Court has general subject matter jurisdiction over this civil action under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the amount in controversy is easily more than $5,000,000 and minimal diversity exists. Specifically, the Data Breach affected tens of thousands of people with damages including reimbursement for out-of-pocket expenses, financial losses from time spent responding to the Data Breach, and the cost of at least seven years of credit monitoring and identity theft protection services. Moreover, minimal diversity exists because Defendant is a citizen of Hawaii and the Data Breach affected patients who are citizens of Vermont, because Defendant notified the Vermont Attorney General of the Data Breach.[5]

13. This Court has personal jurisdiction over Defendant because its headquarters is in this State.

14. Venue is proper in this Court because Plaintiff resides in this District and a substantial portion of the events giving rise to this Action occurred in this District.

## ADDITIONAL FACTUAL ALLEGATIONS

15. The information held by Defendant in its computer systems at the time

[5] Office of the Vermont Attorney General, https://ago.vermont.gov/sites/ago/files/documents/2024-11-06%20Hawaii%20Radiologic%20Associates%20Data%20Breach%20Notice%20to%20Consumers.pdf.

of the Data Breach included the unencrypted PHI of Plaintiff and Class Members.

16. Defendant made promises and representations to Plaintiff and Class Members that their PHI would be kept safe and confidential, and that the privacy of that information would be maintained.

17. Plaintiff's and Class Members' PHI was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

18. Defendant had a duty to adopt reasonable measures to protect the PHI of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PHI safe and confidential.

19. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA" or "FTC Act"), HIPAA, industry standards, and implicit representations made to Plaintiff and Class Members, to keep their PHI confidential and to protect it from unauthorized access and disclosure.

20. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PHI, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PHI from disclosure.

**Defendant's Data Breach Was Imminently Foreseeable**

21. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PHI, like Defendant, preceding the date of the Data Breach.

22. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PHI is valuable and highly sought after by criminal parties who seek to illegally monetize that PHI through unauthorized access.

23. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6]

24. As a custodian of PHI, Defendant knew, or should have known, the importance of safeguarding the PHI entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

25. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the

[6] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s.

PHI of Plaintiff and Class Members from being compromised.

26. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed PHI, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

27. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PHI of Plaintiff and Class Members.

28. The ramifications of Defendant's failure to keep secure the PHI of Plaintiff and Class Members are long lasting and severe. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

**Value of Personally Identifiable Information**

29. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[7] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[8]

30. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[9]

31. The information compromised in the Data Breach is even more significant because it includes health and medical information, which extraordinarily sensitive and private and is commonly used to perpetrate medical and insurance fraud.

32. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[10]

33. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study

[8] *Id.*
[9] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.
[10] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

34. Thus, victims of data breaches must maintain vigilance to protect themselves from the harms associated with data breaches for years to come.

**Defendant Failed to Comply with FTC Guidelines**

35. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

36. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

37. The FTC further recommends that companies not maintain PHI longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the

integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

40. Defendant was at all times fully aware of its obligation to protect the PHI of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

**Defendant Failed to Comply with HIPAA**

41. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

42. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information

Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

43. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

44. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

45. HIPAA requires "comply[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

46. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

47. HIPAA's Security Rule requires defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

48. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

49. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

50. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

51. HIPAA requires a covered entity to have and apply appropriate

sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Pt. 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

52. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

53. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302–164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk

Analysis.

54. Defendant was at all times fully aware of its HIPAA obligations to protect the PHI of consumers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

**Defendant Failed to Comply with Industry Standards.**

55. Experts studying cybersecurity routinely identify institutions that store PHI like Defendant as being particularly vulnerable to cyberattacks because of the value of the PHI which they collect and maintain.

56. Some industry best practices that should be implemented by institutions dealing with sensitive PHI, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all these industry best practices.

57. Other best cybersecurity practices that are standard at large institutions

that store PHI include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

58. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

**Common Injuries & Damages**

59. Because of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PHI ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss

of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to their PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PHI.

**The Data Breach Increases Victims' Risk of Identity Theft.**

60. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' PHI falling into the hands of identity thieves.

61. The unencrypted PHI of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PHI for the express purpose of conducting financial fraud and identity theft operations.

62. Further, the standard operating procedure for cybercriminals is to use some data, like the PHI here, to access "fullz packages" of that person to gain access to the full suite of additional PHI that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's

information to perpetrate even more types of attacks.[12]

63. With "Fullz" packages, cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

64. The development of "Fullz" packages means here that the stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

[12] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

**Loss of Time to Mitigate Risk of Identity Theft and Fraud**

65. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PHI was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

66. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' PHI is affected because such information is commonly used to commit medical and insurance fraud.

67. By spending this time, data breach Plaintiff is not manufacturing his own harm but is taking necessary steps at Defendant's direction and because the Data Breach included his PHI.

68. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for

any indication of fraudulent activity, which may take years to detect.

69. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[13]

70. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[14]

**The Future Cost of Credit and Identity Theft Monitoring**

71. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial

[13] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[14] *See* Fed. Trade Comm'n, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

fraud and identity theft of data breach victims.

72. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

73. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PHI.

**Plaintiff's Experience**

74. Plaintiff provided PHI to Defendant as a condition of receiving medical and healthcare service from Defendant related to injuries.

75. Plaintiff received notice from Defendant that he was affected by the Data Breach.

76. At the time of the Data Breach, Defendant retained Plaintiff's and his minor children's PHI in its system.

77. Plaintiff's PHI was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting PHI.

78. Because of the Data Breach, Plaintiff has suffered a loss of time, interference, and inconvenience because of the Data Breach, including receiving a significant increase in spam phone calls. Plaintiff has also experienced stress and anxiety due to increased concerns for the loss of his privacy.

79. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PHI being placed in the hands of the very people whose mission it is to use that data to steal Plaintiff's identity and to attempt financial fraud.

80. Moreover, the breach of his medical and health information exposes Plaintiff and the Class to a significantly increased risk of medical and health insurance fraud.

81. Critically, the breach of this type of PHI represents a brazen invasion of privacy, which is a harm long recognized in American courts.

## CLASS ALLEGATIONS

82. Plaintiff brings this action on behalf of himself and on behalf of all members of the proposed class defined as:

> All individuals whose PHI was compromised in the Data Breach and to whom Defendant sent an individual notification that they were affected by the Data Breach ("Class").

83. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors,

and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

84. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

85. The proposed Class meets the criteria certification under the Illinois Code of Civil Procedure.

86. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records..

87. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTC Act and/or HIPAA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable

security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard their Private Information;

h. Whether Defendant breached their duties to Class Members to safeguard their Private Information;

i. Whether hackers obtained Class Members' Private Information via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with its clients, which were made expressly for the benefit of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members are entitled to damages;

q. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

88. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia,* all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

89. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent

and experienced in litigating class actions, including data privacy litigation of this kind.

90. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

91. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating her individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the

parties' resources, and protects the rights of each Class Member.

92. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

93. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendant's ability to send those individuals notification letters.

## CLAIMS FOR RELIEF

### COUNT I
### NEGLIGENCE AND NEGLIGENCE PER SE
### (On Behalf of Plaintiff and the Class)

94. Plaintiff incorporates the above allegations as if fully set forth herein.

95. Plaintiff and Class Members provided their non-public PHI to Defendant as a condition of receiving medical and healthcare services.

96. Defendant had full knowledge of the sensitivity of the PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PHI were wrongfully disclosed.

97. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the

information, and to safeguard the information from theft.

98. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

99. Defendant's duty to use reasonable security measures also arose under the common law, and as informed by the FTC Act and HIPAA, which mandates that Defendant implement reasonable cybersecurity measures.

100. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PHI.

101. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

102. Defendant had and continues to have duties to adequately disclose that the PHI of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by third parties.

103. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PHI. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PHI;

b. Allowing unauthorized access to Class Members' PHI;

c. Failing to remove Plaintiff's and Class Members' PHI it was no longer required to retain pursuant to regulations; and

d. Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

104. Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

105. Defendant's violation of the FTC Act and HIPAA also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiff and the proposed Class Members from the harms associated with data

breaches.

106. Defendant has admitted that the PHI of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

107. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the PHI of Plaintiff and Class Members would not have been compromised.

108. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PHI of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

109. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the

continued and certainly increased risk to their PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI.

110. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

111. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PHI in its continued possession.

112. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

113. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendant's

decision not to invest enough resources in its cyber defenses amounts to gross negligence.

**COUNT II**
**BREACH OF IMPLIED CONTRACT**
**(On Behalf of Plaintiff and the Class)**

114. Plaintiff incorporates the above allegations as if fully set forth herein.

115. Plaintiff and the proposed Class Members transferred their PHI to Defendant as part of receiving medical and health services.

116. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their PHI. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members and implicitly agreed to do so.

117. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their PHI as a necessary part of receiving healthcare.

118. Defendant, however, failed to secure Plaintiff and Class Members' PHI and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

119. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PHI, they would not have allowed it to be provided to Defendant.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

invasion of privacy; (ii) theft of their PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI.

## COUNT III
## BREACH OF BAILMENT
## (On Behalf of Plaintiff and the Class)

121. Plaintiff incorporates the above allegations as if fully set forth herein.

122. Plaintiff conveyed his PHI to Defendant lawfully as a condition of receiving medical and health services with the understanding that Defendant would return or delete his PHI when it was no longer required.

123. Defendant accepted this PHI on the implied understanding that Defendant would honor its obligations under federal regulations, state law, and industry standards to safeguard Plaintiff's PHI and act on the PHI only within the confines of the purposes for which Defendant collected Plaintiff's PHI.

124. By accepting Plaintiff's data and storing it on its systems, Defendant had exclusive control over the privacy of Plaintiff's data in that Plaintiff had no control over whether Defendant's copy of Plaintiff's PHI was protected with sufficient safeguards and indeed only Defendant had that control.

125. By failing to implement reasonable cybersecurity safeguards, as detailed above, Defendant breached this bailment agreement causing harm to Plaintiff in the form of violations of his right to privacy and to self-determination of who had/has access to his PHI, in the form of requiring him to spend his own valuable time responding to Defendant's failures, and in the form of forcing Plaintiff and the Class to face years of substantially increased risk of identity theft and financial fraud.

## COUNT IV
## INVASION OF PRIVACY
## (On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates the above allegations as if fully set forth herein.

127. Plaintiff and Class members took reasonable and appropriate steps to keep their PHI confidential from the public.

128. Plaintiff's and Class members' efforts to safeguard their own PHI were successful, as their PHI was not known to the public prior to the Data Breach.

129. Plaintiff and Class members had a legitimate expectation of privacy to their PHI and were entitled to the protection of this information against disclosure

to unauthorized third parties.

130. Defendant owed a duty to its patients, including Plaintiff and the proposed Class Members, to keep their PHI confidential.

131. The unauthorized release of PHI is highly offensive to any reasonable person.

132. Plaintiff's and Class members' PHI is not of legitimate concern to the public.

133. Defendant knew or should have known that Plaintiff's and Class members' PHI was private.

134. Defendant publicized Plaintiff's and Class members' PHI, by communicating it to cybercriminals who had no legitimate interest in this PHI and who had the express purpose of monetizing that information by injecting it into the illicit stream of commerce flowing through the dark web and other malicious channels of communication (e.g., Telegram and Signal).

135. Moreover, because of the ubiquitous nature of data breaches, especially in the healthcare industry, Defendant was substantially certain that a failure to protect PHI would lead to its disclosure to unauthorized third parties, including the thousands of waiting identity thieves who are in a special relationship with Plaintiff and the proposed Class Members—in that those identity thieves are precisely the individuals whose aim it is to misuse such PHI.

136. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that Defendant's inadequate data security measures will likely result in additional data breaches. Plaintiff and Class members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiff's and Class members' privacy by Defendant.

## PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, individually and on behalf of all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to

an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PHI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal

security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xv. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all issues so triable.

Dated: Honolulu, HI, ____December 12, 2024_____.

_____*/s/* Janice D. Heidt_____
Janice D. Heidt
Richard Turbin
J. Gerard Stranch, IV*
Grayson Wells*
Attorneys for Plaintiff and the Proposed Class

*To Seek Pro Hac Vice Admission